REMARKS

Claims 1-20 are currently pending in the application. By this amendment, claim 1 is amended and claims 12-20 are added for the Examiner's consideration. The above amendments and new claims do not add new matter to the application and are fully supported by the original disclosure. For example, support for the amendments and new claims is provided in the claims as originally filed, at Figures 1-3 and 5-9, and at pages 10-16 of the specification. Reconsideration of the rejected claims in view of the above amendments and the following remarks is respectfully requested.

35 U.S.C. §102 Rejection

Claims 1-11 are rejected under 35 U.S.C. §102(b) as being anticipated by Cisco Systems "Network Security: An Executive Overview" (hereinafter referred to as "Cisco"). This rejection is respectfully traversed.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). See MPEP §2131. Applicants submit that the applied art does not show each and every feature of the claimed invention.

This invention relates in general to network security, and more particularly to a method for providing network perimeter security assessment. As opposed to prior art systems in which any given security tool is specific to a single discipline, embodiments of the invention provide a comprehensive network perimeter security assessment. By providing a method for checking network perimeter security that incorporates more than one network security discipline, an

enterprise architecture that is more secure from attacks to computers and network devices may be developed. More specifically, independent claim 1 recites plural reviewing steps and generating a report concerning security of the perimeter *based upon all of the reviewing steps*. By generating a report based upon all of the reviewing steps, the claimed invention provides a comprehensive method for checking network perimeter security. Applicants submit that the applied art does not show at least the feature of generating a report concerning security of the perimeter based upon all of the reviewing steps.

Cisco discloses an overview of aspects of network security and products for providing such security. For example, Cisco discloses: authentication systems for authenticating users and determining access levels (page 3); firewalls for providing a barrier to traffic crossing a network perimeter (page 4); network vulnerability scanners for proactively identifying areas of weakness (page 4); and intrusion detection systems for monitoring and responding to security events as they occur (page 4).

However, Cisco does not disclose plural reviewing steps and generating a report concerning security of the perimeter based upon all of the reviewing steps. Instead, each of the systems disclosed by Cisco operates in relative isolation from the other systems. And there is simply no disclosure or suggestion in Cisco of generating a report concerning security of the perimeter based upon all of the steps of: *(i)* reviewing security of a network perimeter architecture, *(ii)* reviewing security of data processing devices that transfer data across the perimeter of the network, *(iii)* reviewing security of applications that transfer data across said perimeter, and *(iv)* reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter.

Moreover, Cisco only discloses security system components. However, Cisco does not disclose reviewing the security of these components. Applicants respectfully submit that merely describing a security component does not explicitly or implicitly disclose reviewing the security of aspects of a network perimeter, as required by claim 1. Therefore, Cisco does not disclose *(i)* reviewing security of a network perimeter architecture, *(ii)* reviewing security of data processing devices that transfer data across the perimeter of the network, *(iii)* reviewing security of applications that transfer data across said perimeter, and *(iv)* reviewing vulnerability of applications or data processing devices within said perimeter from computers or users outside of said perimeter, as recited in claim 1.

As such, Cisco does not disclose all of the features of the claimed invention, and does not anticipate claim 1. Moreover, claims 2-11 depend from claim 1, and are distinguishable from Cisco at least for the reasons discussed above with respect to claim 1.

Furthermore, claims 2-11 recite additional features that are not disclosed or suggested by Cisco. For example, Cisco does not disclose reviewing security of data processing devices within said perimeter that authenticate computers or users outside of said perimeter that request to access an application within said perimeter, as recited in claim 2. The Examiner asserts that Cisco discloses this feature via the Cisco Secure Access Control Server (ACS) at page 3. Applicants respectfully disagree. The ACS provides a foundation to authenticate users, determine access levels, and archive audit and accounting data. This description makes no mention of *reviewing* the security of data processing devices. Instead, Cisco merely describes authentication features associated with a user identity security tool; however, none of the features includes *reviewing* the security of data processing devices.

Accordingly, Applicants respectfully request that the §102 rejection of claims 1-11 be withdrawn.

Added Claims

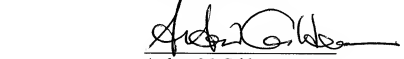
By this amendment, new claims 12-20 are added and are believed to be distinguishable from the applied art and in condition for allowance. Claims 12-15 depend from allowable claim 1, are allowable for the reasons discussed above with respect to claim 1, and additionally recite features that are not disclosed or suggested by the applied art. For example, the applied art does not disclose: categorizing components as either control points or non-control points, as recited in claim 12; testing control points with port scans and testing control points with penetration tests, as recited in claim 13; performing a policy review of an enterprise which owns or controls said network, and defining review parameters based upon the policy review, as recited in claim 14; or the reviewing security of a network perimeter architecture comprises receiving review parameters from a policy review and generating test cases, and the reviewing security of data processing devices that transfer data across the perimeter of the network comprises receiving the review parameters, receiving the test cases, and performing the test cases, as recited in claim 15.

New claims 16-20 are distinguishable from the applied art at least for the reason that each of these claims recites generating a report concerning security of said perimeter based upon a plurality of reviews.

CONCLUSION

In view of the foregoing amendments and remarks, Applicants submit that all of the claims are patentably distinct from the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue. The Examiner is invited to contact the undersigned at the telephone number listed below, if needed. Applicants hereby make a written conditional petition for extension of time, if required. Please charge any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 09-0457.

Respectfully submitted,
W. Carey BUNN et al.



Andrew M. Calderon
Registration No. 38,093

June 28, 2007
Greenblum & Bernstein, P.L.C.
1950 Roland Clarke Place
Reston, Virginia 20191
Telephone: 703-716-1191
Facsimile: 703-716-1180